ABSTRACT

A signal transmitted from a first device to a second device is encrypted using an encryption key generated from a preceding part of the signal itself. The signal is decrypted in the second device using a decryption key generated from a preceding part of the received and decrypted signal. This encryption method provides effective privacy protection, because the encryption and decryption keys are constantly changing. Since the transmitted signal provides its own encryption and decryption keys, the method is inexpensive to implement, and can be used in systems such as packet transmission systems that transmit signals intermittently.